communication means for receiving an e-mail attachment from the network; and

processing means for converting the e-mail attachment from an executable format to a non-executable format by using one of a plurality of conversion processes selected in accordance with a type of the e-mail message, the non-executable format retaining an appearance, human readability and semantic content of the e-mail message and for returning the e-mail attachment to the network.

35. (Amended) The sacrificial server of claim 31, wherein the sacrificial server stores a list of approved attachment file types and extensions, determines whether the attachment is of a file type or extension which is in the list of approved attachment file types and extensions, and, if the attachment is not of a file type or extension which is in the list of approved attachment file types and extensions, and informs the network that a message containing a non-approved attachment has been received.

Please add the following new claims:

--42. The method of claim 5, wherein the plurality of sacrificial servers are separate from the gatekeeper server.

43. The system of claim 20, wherein the plurality of sacrificial servers are separate from the gatekeeper server.--

REMARKS

At the outset, the Applicants acknowledge with appreciation the courtesy extended by the Examiner and her Supervisory Primary Examiner during the personal interview conducted January 30, 2003.

The Office Action dated December 18, 2002, and the Supplemental Office Action dated February 6, 2003, have been carefully considered. In response thereto, the present application

has been amended in a manner that is believed to place it into condition for allowance. Accordingly, reconsideration and withdrawal of the outstanding Office Action is respectfully solicited.

In response to the objection to the drawings, the Applicants respectfully submit that the proposed drawing corrections set forth in the Request for Drawing Change Approval filed concurrently herewith overcome that objection.

Furthermore, in response to the rejection of claims 1, 4, 16, 19 and 31 under 35 U.S.C. §103(a), the Applicants respectfully submit that the invention as now claimed in claims 1, 4, 16, 19 and 31 would not have been obvious over *Chen et al* in view of *Templeton et al* and *Newton's Telecom Dictionary.*

According to the present claimed invention, the e-mail message is converted from an executable format to a non-executable format by using one of a plurality of conversion processes selected in accordance with a type of the e-mail message. The non-executable format retains an appearance, human readability and semantic content of the e-mail message. That feature was discussed during the interview and is supported in the originally filed specification, e.g., from page 5, line 14, through page 7, line 18. That technique achieves two goals that in the prior art appeared to be desirable but mutually exclusive. That is, the recipient of the e-mail message is protected from viruses or other malicious code while still being able to see, in a timely fashion, any human-readable content for which the e-mail message was sent in the first place.

As only one illustrative example, an attachment in Microsoft Word format can be converted to Adobe Acrobat (PDF) format. Thus, while the recipient can still read the attachment, any macro viruses in the Microsoft Word file are disabled. The ability of the user to read the PDF file is important because the e-mail message may contain time-sensitive

information whose arrival would be needlessly delayed if the attachment were simply quarantined, scrambled, or deleted.

As a further advantage, the conversion is done in accordance with an original data format of the message (e.g., using standard Windows application processing, as taught in the originally filed specification, page 7, lines 11-12). Thus, the present claimed invention can be used with e-mail messages in multiple formats (e.g., Word and Excel).

The Office Action acknowledges that *Chen et al* does not teach or suggest the conversion of executable code from an executable format to a non-executable format. Instead, the Office Action relies on *Templeton* for that teaching. However, as will be explained, the combination of references suggested in the Office Action would still not have resulted in, taught, or suggested the above-mentioned features of the present claimed invention.

Templeton teaches a method for scrambling the contents of a file, thus rendering it non-executable. The reference suggests forwarding the scrambled file to a user while scrambled.

However, the scrambling of *Templeton* has the following deficiencies with regard to the present claimed invention. A scrambled file does not retain an appearance, human readability and semantic content of the e-mail message. Instead, a user who receives it simply receives a scrambled file, which, of course, has no perceivable content. If the user wants to read the content of the file, the user must unscramble it. Of course, if the unscrambled file contains a virus, the user is back where she would have been if the virus-infected file had simply been sent to her. The present claimed invention avoids such an unfortunate result, since the user can see the content, if any, without having to restore a virus-infected file.

Furthermore, the present claimed invention permits the user-readable content to be preserved by converting in accordance with an original data format of the e-mail message.

Templeton teaches or suggests no such thing, but simply scrambles files.

The Office Action cites *Newton's Telecom Dictionary* only for a definition of a gatekeeper server. Thus, *Newton's Telecom Dictionary* does not overcome the above-noted deficiencies of *Chen et al* and *Templeton*.

For the reasons set forth above, even if the references were combined in the manner proposed in the Office Action, they would not have resulted in, taught, or even remotely suggested the present claimed invention. Therefore, the Applicants respectfully submit that the present claimed invention would not have been obvious over that combination of references.

Moreover, in response to the rejection of the remaining claims under 35 U.S.C. §103(a), the Applicants respectfully submit that none of the other applied references would have overcome the above-noted deficiencies of *Chen et al, Templeton* and *Newton's Telecom Dictionary*. Therefore, since each of the remaining claims depends from one of claims 1, 16 and 31, the Applicants respectfully submit that the remaining grounds of rejection are moot.

Finally, the dependent claims reciting a plurality of sacrificial servers in communication with the gatekeeper server provide a further basis for distinguishing the present invention over the applied prior art. The use of a plurality of sacrificial servers allows the system to remain operational even if a virus takes down one of the sacrificial servers. The Office Action cites *Schnurer et al* for teaching of a sacrificial server. However, that reference merely teaches a virus trapping device that creates a virtual world for the virus. When multiple trapping devices are taught at all, they are merely shown in one-to-one correspondence with nodes (gatekeeper servers), with each trapping device in communication with only one node. Thus, the combination of *Schnurer et al* with the other applied references would not have taught or suggested the subject matter of those claims which recite a plurality of sacrificial servers in

communication with the gatekeeper server.

For the reasons set forth above, the Applicants respectfully submit that the subject matter of the present claims would not have been obvious over any of the combinations of references applied in the Office Action. Therefore, the Applicants respectfully traverse all grounds of rejection under 35 U.S.C. §103(a).

As all grounds of objection and rejection have been addressed and overcome, the Applicants respectfully request reconsideration and withdrawal of the outstanding Office Action and issuance of a Notice of Allowance of claims 1-43 as now submitted.

In the event there are any questions relating to this Response or to the application in general, it would be appreciated if the Examiner would telephone the undersigned attorney concerning such questions so that prosecution of this application may be expedited

Please charge any shortage of fees or credit any overpayment thereof to BLANK ROME LLP, Deposit Account No. 23-2185 (109933-00103). In the event that a separate Petition for an Extension of Time does not accompany this submission or does not suffice to render this submission timely, the Applicants herewith petition under 37 C.F.R. §1.136(a) for an extension of time for as many months as are required to render this submission timely. Any fee due is authorized above.

Respectfully submitted,

Walter Mason STEWART et al.

By:_____
David J. Edmondson
Reg. No. 35,126

BLANK ROME LLP
900 17th Street, N.W., Suite 1000
Washington, D.C. 20006
Phone: (202) 530-7400
Fax: (202) 463-6915

AMENDED CLAIMS MARKED TO SHOW CHANGES

1. (Amended) A method for protecting a network from a virus contained in an e-mail message as executable code, the method comprising:

(a) receiving the e-mail message in a gatekeeper server;

(b) converting the [executable code] e-mail message from an executable format to a non-executable format by using one of a plurality of conversion processes selected in accordance with a type of the e-mail message, the non-executable format retaining an appearance, human readability and semantic content of the e-mail message; and

(c) forwarding the non-executable format to the recipient of the e-mail message.

5. (Amended) The method of claim 4, wherein step (b) comprises:

(i) providing a plurality of sacrificial servers in communication with the gatekeeper server;

(ii) forwarding the attachment from the gatekeeper server to [a] one of the plurality of sacrificial [server] servers; and

[(ii)] (iii) converting the attachment to the non-executable format on said one of the plurality of sacrificial [server] servers by using said one of the plurality of conversion processes selected in accordance with the type of the e-mail message, the non-executable format retaining the appearance, human readability and semantic content of the e-mail message.

9. (Amended) The method of claim 4, wherein step (b) comprises:

(i) maintaining a list of approved attachment file types and extensions;

(ii) determining whether the attachment is of a type or extension which is in the list of approved attachment file types and extensions; and

(iii) if the attachment is not of a type or extension which is in the list of approved

attachment file types and extensions, informing the recipient that a message containing a non-approved attachment has been received.

16. (Amended) A system for protecting a network from a virus contained in an e-mail message as executable code, the system comprising:

a workstation computer on the network used by [an] a recipient of the e-mail message;

a gatekeeper server, in communication with the workstation computer over the network, for receiving the e-mail message; and

a computer on the network for converting the [executable code] e-mail message from an executable format to a non-executable format by using one of a plurality of conversion processes selected in accordance with a type of the e-mail message, the non-executable format retaining an appearance, human readability and semantic content of the e-mail message and forwarding the [non-executable format] converted e-mail message to the workstation computer.

20. (Amended) The system of claim 16, wherein the computer for converting is one of a plurality of sacrificial [server which is separate from the gatekeeper server] servers which are in communication with the gatekeeper server.

21. (Amended) The system of claim 20, wherein the plurality of sacrificial [server is] servers are examined for virus activity.

22. (Amended) The system of claim 21, wherein the network further comprises a read-only device, and wherein the sacrificial [server is] servers are rebooted from a safe copy of an operating system obtained from the read-only device.

23. (Amended) The system of claim 20, wherein communications between the gatekeeper server and the sacrificial [server] servers are authenticated using a challenge-and-response technique.

24. (Amended) The system of claim 16, wherein the network maintains a list of approved attachment file types and extensions, determines whether the attachment is of a file type or extension which is in the list of approved attachment file types and extensions, and, if the attachment is not of a file type or extension which is in the list of approved attachment file types and extensions, informs the recipient that a message containing a non-approved attachment has been received.

31. (Amended) A sacrificial server for use on a network, the sacrificial server comprising:

communication means for receiving an e-mail attachment from the network; and

processing means for converting the e-mail attachment from an executable format to a non-executable format by using one of a plurality of conversion processes selected in accordance with a type the e-mail message, the non-executable format retaining an appearance, human readability and semantic content of the e-mail message and for returning the e-mail attachment to the network.

35. (Amended) The sacrificial server of claim 31, wherein the sacrificial server stores a list of approved attachment file types and extensions, determines whether the attachment is of a file type or extension which is in the list of approved attachment file types and extensions, and, if the attachment is not of a file type or extension which is in the list of approved attachment file types and extensions, and informs the network that a message containing a non-approved attachment has been received.